

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-318887

(43)Date of publication of application : 07.11.2003

(51)Int.Cl. H04L 9/32  
G06F 15/00  
G09C 1/00

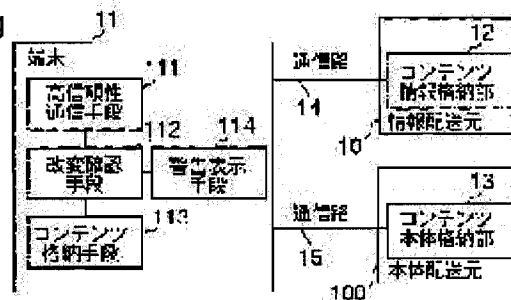
(21)Application number : 2002-123831 (71)Applicant : NEC CORP  
(22)Date of filing : 25.04.2002 (72)Inventor : USUI KAZUTOSHI

(54) CONTENTS DISTRIBUTION SYSTEM, ITS METHOD AND CONTENTS RECEIVING TERMINAL

(57)Abstract:

PROBLEM TO BE SOLVED: To realize the safe distribution of contents without using highly reliable technology and to reduce operating problems and costs.

SOLUTION: Since only contents information for checking whether the body of contents is modified or not is received from a highly reliable communication line and the body of contents can be acquired from a normal communication line, the contents distribution system does not require specific processing for securing reliability.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2003-318887  
(P2003-318887A)

(43) 公開日 平成15年11月7日 (2003. 11. 7)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	ターミナル* (参考)
H 0 4 L 9/32		C 0 6 F 15/00	3 3 0 Z 5 B 0 8 J
G 0 6 F 15/00	3 3 0	C 0 9 C 1/00	6 4 0 D 5 J 1 0 4
G 0 9 C 1/00	6 4 0		6 5 0 Z
	6 5 0	H 0 4 L 9/00	6 7 5 A

審査請求 未請求 請求項の数24 O L (全 7 頁)

(21) 出願番号 特願2002-123831 (P2002-123831)

(22) 出願日 平成14年4月25日 (2002. 4. 25)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 白井 和敏

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100109313

弁理士 机 昌彦 (外2名)

Fターム(参考) 5B085 AE29 BA06 BG03 BC04 BG07

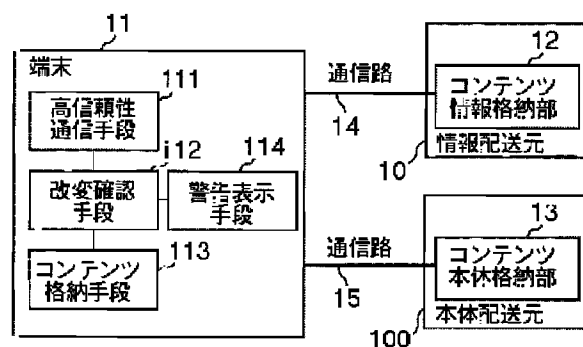
5J104 AA12 NA12 PA07 PA14

(54) 【発明の名称】 コンテンツ配送システム、方法およびコンテンツ受信端末

(57) 【要約】

【課題】 従来コンテンツ配送処理は、コンテンツ本体に暗号技術を用いた署名等による高信頼性技術が使用されていたため、鍵発行主体をどうするか、あるいは公開鍵基盤をどのように構築するかなど運用面での問題があり、また処理量が増大しコストが大きかった。

【解決手段】 本発明に係るコンテンツ配送システムは、コンテンツ本体の改変の有無を確認するためのコンテンツ情報のみ高信頼性通信路から受信することにより、コンテンツ本体は通常の通信路で入手することが可能となり、信頼性確保のため特別な処理を必要としない。



## 【特許請求の範囲】

【請求項1】 少なくとも1つのコンテンツ情報を受信するための高信頼性通信手段と、コンテンツ本体改変の有無を判断する改変確認手段とからなり、前記受信したコンテンツ情報に基づきコンテンツ本体が改変されたか否かの確認を行うことを特徴とするコンテンツ配送システム。

【請求項2】 前記コンテンツ情報はコンテンツ本体を一方方向性ハッシュ関数を用いて予め計算されたコンテンツ本体に関するハッシュ期待値を含むことを特徴とする請求項1記載のコンテンツ配送システム。

【請求項3】 前記コンテンツ情報はコンテンツ本体の位置情報を含むことを特徴とする請求項1または請求項2記載のコンテンツ配送システム。

【請求項4】 請求項1乃至請求項3のコンテンツ配送システムにおいて、前記改変確認手段により改変されたことが確認された場合は警告を行うことを特徴とするコンテンツ配送システム。

【請求項5】 少なくとも1つのコンテンツ情報を受信するための高信頼性通信手段を有する通信センタと、前記通信センタと高信頼性通信手段により接続されコンテンツ本体改変の有無を判断する改変確認手段を有する端末とからなり、前記通信センタは前記コンテンツ情報および前記コンテンツ本体を受信した後前記高信頼性通信手段により前記端末に送信し、前記端末の改変確認手段は受信した前記コンテンツ情報に基づき前記コンテンツ本体が改変されたか否かの確認を行うことを特徴とするコンテンツ配送システム。

【請求項6】 前記コンテンツ情報はコンテンツ本体を一方方向性ハッシュ関数を用いて予め計算されたコンテンツ本体に関するハッシュ期待値を含むことを特徴とする請求項5記載のコンテンツ配送システム。

【請求項7】 前記コンテンツ情報はコンテンツ本体の位置情報を含むことを特徴とする請求項5または請求項6記載のコンテンツ配送システム。

【請求項8】 請求項5乃至請求項7のコンテンツ配送システムにおいて、前記改変確認手段により改変されたことが確認された場合は警告を行うことを特徴とするコンテンツ配送システム。

【請求項9】 少なくとも1つのコンテンツ情報を受信するための高信頼性通信手段と、前記受信したコンテンツ情報により別途受信したコンテンツ本体が改変されたか否かを確認する改変確認手段を有することを特徴とするコンテンツ受信端末。

【請求項10】 前記コンテンツ情報はコンテンツ本体を一方方向性ハッシュ関数を用いて予め計算されたコンテンツ本体に関するハッシュ期待値を含むことを特徴とする請求項9記載のコンテンツ受信端末。

【請求項11】 前記コンテンツ情報はコンテンツ本体

の位置情報を含むことを特徴とする請求項9または請求項10記載のコンテンツ受信端末。

【請求項12】 請求項9乃至請求項11のコンテンツ受信端末において、前記改変確認手段により改変されたことが確認された場合は警告を行うことを特徴とするコンテンツ受信端末。

【請求項13】 少なくとも1つのコンテンツ本体および高信頼性通信手段により受信した少なくとも1つのコンテンツ情報を通信センタから受信するための高信頼性通信手段と、

前記コンテンツ情報に基づき前記コンテンツ本体が改変されたか否かの確認を行うための改変確認手段を有することを特徴とするコンテンツ受信端末。

【請求項14】 前記コンテンツ情報はコンテンツ本体を一方方向性ハッシュ関数を用いて予め計算されたコンテンツ本体に関するハッシュ期待値を含むことを特徴とする請求項13記載のコンテンツ受信端末。

【請求項15】 前記コンテンツ情報はコンテンツ本体の位置情報を含むことを特徴とする請求項13または請求項14記載のコンテンツ受信端末。

【請求項16】 請求項13乃至請求項15のコンテンツ受信端末において、前記改変確認手段により改変されたことが確認された場合は警告を行うことを特徴とするコンテンツ受信端末。

【請求項17】 少なくとも1つのコンテンツ情報を高信頼性通信手段により受信し、前記コンテンツ情報に基づきコンテンツ本体が改変されたか否かを確認することを特徴とするコンテンツ配送方法。

【請求項18】 前記コンテンツ情報はコンテンツ本体を一方方向性ハッシュ関数を用いて予め計算されたコンテンツ本体に関するハッシュ期待値を含むことを特徴とする請求項17記載のコンテンツ配送方法。

【請求項19】 前記コンテンツ情報はコンテンツ本体の位置情報を含むことを特徴とする請求項17または請求項18記載のコンテンツ配送方法。

【請求項20】 請求項17乃至請求項19のコンテンツ配送方法において、前記改変確認手段により改変されたことが確認された場合は警告を行うことを特徴とするコンテンツ配送方法。

【請求項21】 通信センタは少なくとも1つのコンテンツ本体格納部および高信頼性通信手段により接続された少なくとも1つのコンテンツ情報格納部からコンテンツ本体およびコンテンツ情報を受信し、コンテンツ受信端末は前記通信センタから高信頼性通信手段により前記コンテンツ本体およびコンテンツ情報を受信し、前記コンテンツ情報に基づき前記コンテンツ本体が改変されたか否かの確認を行うことを特徴とするコンテンツ配送方法。

【請求項22】 前記コンテンツ情報はコンテンツ本体を一方方向性ハッシュ関数を用いて予め計算されたコンテンツ本体に関するハッシュ期待値を含むことを特徴とする請求項21記載のコンテンツ配送方法。

【請求項23】 前記コンテンツ情報はコンテンツ本体の位置情報を含むことを特徴とする請求項21または請求項22記載のコンテンツ配送方法。

【請求項24】 請求項21乃至請求項23のコンテンツ配送方法において、前記改変確認手段により改変されたことが確認された場合は警告を行うことを特徴とするコンテンツ配送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、改変のない安全なプログラム等のコンテンツ（デジタルデータ）を適正な処置により入手するためのコンテンツの配送に関する。

【0002】

【従来の技術】従来のコンテンツ配送では、信頼性の低い通信路を通して配送されたコンテンツはそれ自体信頼性が低く安全ではないとの前提のもとに、第三者による盗聴あるいは改竄がおこなわれることを防止するため、暗号技術を用いた署名等による高信頼性技術が使用されていた。従来から用いられていたコンテンツ配送時の具体的な盗聴・改竄防止策には、特願平11-99745の公開公報等で開示されている通り、以下のようなものがある。

【0003】（方法1）送信側装置が受信側装置の暗号鍵を取得し、コンテンツに含まれるすべてのデータを受信側装置の暗号鍵で暗号化して転送する。したがって受信側装置はコンテンツ本体も含めすべてのデータをその装置の暗号鍵で暗号化された状態で蓄積する。

【0004】（方法2）コンテンツ管理データ等は暗号化せず、コンテンツ本体は暗号化された状態で転送・蓄積を行う。暗号化はコンテンツ配信装置（コンテンツの作成・配信を行う装置）で一元的に行う。コンテンツ本体の暗号鍵はコンテンツごとに固有のものとする。コンテンツ管理データに対してはコンテンツ配信装置においてデジタル署名を作成する。コンテンツ転送時、送信側装置において受信側装置の暗号鍵を取得し、コンテンツ本体の暗号鍵を受信側装置の暗号鍵で暗号化し、コンテンツ管理データ、コンテンツ管理データのデジタル署名、暗号化されたコンテンツ本体と共に転送する。

【0005】（方法3）上記方法2において暗号化されていないコンテンツ管理データと暗号化されたコンテンツ本体の全体に対してデジタル署名を作成し、コンテンツ管理データ、暗号化されたコンテンツ本体と共に転送する。

【0006】

【発明が解決しようとする課題】従来の署名処理は、鍵発行主体をどうするか、あるいは公開鍵基盤をどのよう

に構築するかなど運用面で煩雑な手続きが必要であり、また処理量が増大しコストが大きくなるという問題があった。本発明は公衆回線やスクランブルされたデジタル回線など信頼性の高い通信路（高信頼性通信路）でインターネットプロバイダや携帯電話事業者と接続されている端末が多いことを利用して、前述の問題点となる技術を使用しないで安全にコンテンツを配送するものである。

【0007】

【課題を解決するための手段】本発明は、上記の課題を解決し、高信頼性技術を使用せずにコンテンツの安全な配送を実現し、運用面の問題およびコストの低減を図ることを目的とする。

【0008】本発明に係るコンテンツ配送システムは、少なくとも1つのコンテンツ情報（コンテンツ本体の改変の有無を判断するためのデータ）を受信するための高信頼性通信手段（送受信されるデータに暗号化、スクランブル等の処理を行うことにより、または、専用線等を通信路として使用することにより通信路内でデータの改変がなされるおそれの極めて低い通信手段）とコンテンツ本体改変の有無を判断する改変確認手段からなり、前記受信したコンテンツ情報に基づきコンテンツ本体が改変されたか否かの確認を行うことを特徴とする。

【0009】さらに、前記コンテンツ配送システムはコンテンツ情報がコンテンツ本体を一方方向性ハッシュ関数を用いて予め計算されたコンテンツ本体に関するハッシュ期待値を含むことを特徴とする。

【0010】さらに、前記コンテンツ配送システムはそのコンテンツ情報がコンテンツ本体の位置情報を含むことを特徴とする。

【0011】さらに、前記コンテンツ配送システムは、前記改変確認手段により改変されたことが確認された場合は警告を行うことを特徴とする。

【0012】また、本発明に係るコンテンツ配送システムは、少なくとも1つのコンテンツ情報を受信するための高信頼性通信手段を有する通信センタと前記通信センタと高信頼性通信手段により接続されコンテンツ本体改変の有無を判断する改変確認手段を有する端末からなり、前記通信センタは前記コンテンツ情報および前記コンテンツ本体を受信した後前記高信頼性通信手段により前記端末に送信し、前記端末の改変確認手段は受信した前記コンテンツ情報に基づき前記コンテンツ本体が改変されたか否かの確認を行うことを特徴とする。

【0013】さらに、前記コンテンツ配送システムはコンテンツ情報がコンテンツ本体を一方方向性ハッシュ関数を用いて予め計算されたコンテンツ本体に関するハッシュ期待値を含むことを特徴とする。

【0014】さらに、前記コンテンツ配送システムはそのコンテンツ情報がコンテンツ本体の位置情報を含むことを特徴とする。

【0015】さらに、前記コンテンツ配送システムは、前記改変確認手段により改変されたことが確認された場合は警告を行うことを特徴とする。

【0016】また、本発明に係るコンテンツ受信端末は、少なくとも1つのコンテンツ情報を受信するための高信頼性通信手段と前記受信したコンテンツ情報により別途受信したコンテンツ本体が改変されたか否かを確認する改変確認手段を有することを特徴とする。

【0017】さらに、前記コンテンツ受信端末は、前記コンテンツ情報がコンテンツ本体を一方方向性ハッシュ関数を用いて予め計算されたコンテンツ本体に関するハッシュ期待値を含むことを特徴とする。

【0018】さらに、前記コンテンツ受信端末は、前記コンテンツ情報がコンテンツ本体の位置情報を含むことを特徴とする。

【0019】さらに、前記コンテンツ受信端末は、前記改変確認手段により改変されたことが確認された場合は警告を行うことを特徴とする。

【0020】また、本発明に係るコンテンツ受信端末は、少なくとも1つのコンテンツ本体および高信頼性通信手段により受信した少なくとも1つのコンテンツ情報を通信センタから受信するための高信頼性通信手段と前記コンテンツ情報に基づき前記コンテンツ本体が改変されたか否かの確認を行うための改変確認手段を有することを特徴とする。

【0021】さらに、前記コンテンツ受信端末は、前記コンテンツ情報がコンテンツ本体を一方方向性ハッシュ関数を用いて予め計算されたコンテンツ本体に関するハッシュ期待値を含むことを特徴とする。

【0022】さらに、前記コンテンツ受信端末は、前記コンテンツ情報がコンテンツ本体の位置情報を含むことを特徴とする。

【0023】さらに、前記コンテンツ受信端末は、前記改変確認手段により改変されたことが確認された場合は警告を行うことを特徴とする。

【0024】また、本発明に係るコンテンツ配送方法は、少なくとも1つのコンテンツ情報を高信頼性通信手段により受信し、前記コンテンツ情報に基づきコンテンツ本体が改変されたか否かを確認することを特徴とする。

【0025】さらに、前記コンテンツ配送方法は、前記コンテンツ情報がコンテンツ本体を一方方向性ハッシュ関数を用いて予め計算されたコンテンツ本体に関するハッシュ期待値を含むことを特徴とする。

【0026】さらに、前記コンテンツ配送方法は、前記コンテンツ情報がコンテンツ本体の位置情報を含むことを特徴とする。

【0027】さらに、前記コンテンツ配送方法は、前記改変確認手段により改変されたことが確認された場合は警告を行うことを特徴とする。

【0028】また、本発明に係るコンテンツ配送方法は、通信センタが少なくとも1つのコンテンツ本体格納部および高信頼性通信手段により接続された少なくとも1つのコンテンツ情報格納部からコンテンツ本体およびコンテンツ情報を受信し、コンテンツ受信端末は前記通信センタから高信頼性通信手段により前記コンテンツ本体およびコンテンツ情報を受信し、前記コンテンツ情報に基づき前記コンテンツ本体が改変されたか否かの確認を行うことを特徴とする。

【0029】さらに、前記コンテンツ配送方法は、前記コンテンツ情報がコンテンツ本体を一方方向性ハッシュ関数を用いて予め計算されたコンテンツ本体に関するハッシュ期待値を含むことを特徴とする。

【0030】さらに、前記コンテンツ配送方法は、前記コンテンツ情報がコンテンツ本体の位置情報を含むことを特徴とする。

【0031】さらに、前記コンテンツ配送方法は、前記改変確認手段により改変されたことが確認された場合は警告を行うことを特徴とする。

【0032】このようにコンテンツ情報格納部とコンテンツ本体格納部を分離し、別々に受信することおよび一方方向性ハッシュアルゴリズムの使用等により改変のないことを確認することができるため、安全にコンテンツを配送することを可能となる。

【0033】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【0034】図1は本発明の一実施例の構成図である。本発明のコンテンツ配送の一実施例は、コンテンツ情報格納部12をもつ情報配送元10と、コンテンツ本体格納部13をもつ本体配送元100と、コンテンツの配送を受ける 端末11から構成されている。そして、 端末11とコンテンツ情報配送装置12とは、通信路14で、 端末11とコンテンツ本体配送装置13とは、通信路15で結ばれている。

【0035】さらに 端末11は、高信頼性通信手段111、改変確認手段112、コンテンツ格納手段113、および警告表示手段114から構成されている。高信頼性通信手段111は、コンテンツ情報格納部12と通信し信頼性の高いデータを取得する。

【0036】改変確認手段112は、一方方向性ハッシュアルゴリズムを用いて、コンテンツ本体のハッシュ値を計算しコンテンツ情報内に格納されている期待値と比較する。

【0037】コンテンツ格納手段113は、コンテンツ情報およびコンテンツ本体の格納や破棄を行う。

【0038】警告表示手段114は、改変確認手段112で改変があったと認められた場合に、端末利用者に対する旨を表示する。

【0039】

【実施例】次に、図1及び図2のフローチャートを参照して本実施例の全体の動作について詳細に説明する。

【0040】まず、受信したいコンテンツのコンテンツ情報および必要な場合はコンテンツ本体の格納先リンク情報を入手し、高信頼性通信手段111により、情報配送元10からコンテンツ情報を受信する(図2のステップA1)。高信頼性通信手段とは、送受信されるデータに暗号化、スクランブル等の処理を行うことにより、通信路内でデータの改変がなされるおそれの極めて低い通信手段を意味する。

【0041】コンテンツ情報には、ハッシュ期待値およびシステムによってはコンテンツ本体の格納先リンク情報が格納されている。

【0042】次に、コンテンツ情報に格納先リンク情報が格納されている場合は、格納先リンク情報から格納先を知り、通信路15を通じてコンテンツ本体を入手する。通信路15は、公衆回線や専用回線、スクランブルされたデジタル無線通信路を用いた高信頼性通信手段でも、インターネット等を用いた信頼性の低い通信手段でもよい。(ステップA2)。

【0043】さらに、情報配送元10と本体配送元100が同じ主体かどうかを比較する(ステップA3)。

【0044】比較した結果、同じであれば、コンテンツ情報がコンテンツ本体の改変にあわせて改変されているおそれがあるため、処理を中止する。そうでなければ処理を継続する。(ステップ4)。

【0045】一方向性ハッシュ関数を用いてコンテンツ本体のハッシュ値を計算し(ステップ5)、ステップAで入手したコンテンツ情報に格納されている期待値と比較する(ステップ6)。

【0046】期待値と一致していれば、改変されていない安全なコンテンツであると認め、コンテンツ格納手段113を用いてコンテンツを端末内に格納する(ステップA9)。

【0047】そうでなければ、警告表示手段114を用いて、その旨を端末利用者に通知する(ステップA8)次に、本発明の他の実施例について図面を参照して説明する。

【0048】コンテンツ情報格納部が1つの場合で説明してきたが、コンテンツ情報格納部は、複数に拡張可能である。コンテンツ情報とコンテンツ本体の関係は、コンテンツ情報内に格納先情報として記述されているため、コンテンツ本体格納部の数は、コンテンツ情報格納部に依存しない。図3は、コンテンツ情報格納部がN個の場合の例である。通信事業者が通信事業者内にコンテンツ情報配送装置をもち、コンテンツ提供者がコンテンツ本体を管理し、インターネットを通じて端末にコンテンツ本体を配送するのがこの例にあたる。

【0049】さらに、上記実施例では、通信路はコンテンツ情報の受信用およびコンテンツ本体受信用の少なく

とも2つの通信路が構成に含まれているが、特にこのような限定をせず1つの通信路において、コンテンツ情報のみ高信頼性通信手段を使って受信することにより本発明の目的を達成するという実施例が考えられる。

【0050】さらに、他の実施例について説明する。図4は携帯電話等の無線端末が通信センタを介してコンテンツを入手するシステムの構成図である。無線端末においては、端末と通信センタとの間で送受信される全てのデータは高信頼性通信手段によりスクランブル処理等されており、通信路47は信頼性の高い通信路である。また、通信センタがコンテンツ情報を受信するための通信路44は高信頼性通信手段が使用されるかまたは専用線等を使用しているため信頼性の高い通信路となっている。ここで、まず、端末41が必要とするコンテンツを通信センタ46に要求すると要求を受けた通信センタ46は、コンテンツ情報を予め登録しているコンテンツ登録センタ40にアクセスし、コンテンツ情報を信頼性の高い通信路44から受信する。その後、通信センタはコンテンツ情報に格納されている格納先リンク情報から要求されているコンテンツを扱っているコンテンツサーバ400を探し、インターネット経由でコンテンツ本体をコンテンツ本体格納部43から受信する。通信センタは、受信したコンテンツ情報に格納されたハッシュ期待値およびコンテンツ本体を信頼性の高い通信路47で端末に送信する。端末41が受信したハッシュ期待値は通信路44および47を通して受信されるため信頼性の高いデータであるが、コンテンツ本体は通信路45がインターネット等の信頼性の低いものであるため、改変された可能性がある。しかし、上記の通り受信したハッシュ期待値は改変の可能性のないものであるため、端末41は改変確認手段によりコンテンツ本体が改変されているか否かを判断することができる。

【0051】また、通信事業者が内部にコンテンツ情報配送装置をもつことにより、端末とコンテンツ情報配送装置は、信頼のおける通信路で接続されることが可能である。

【0052】さらに、上記実施例ではいずれもハッシュ関数により一方向性の期待値を算出し、これを改変の有無の確認に使用しているが、他の関数等による処理で期待値からコンテンツ本体が推測できないものを使用する実施例も考えられる。

【0053】

【発明の効果】第1の効果としては、コンテンツをコンテンツ情報部とコンテンツ本体部に分離し、コンテンツ情報部を信頼性の高い高信頼性通信路を使用し端末側に配送するため、デジタル認証や公開鍵基盤などを用いずに安全にコンテンツを配送することが可能となる。

【0054】第2の効果としては、コンテンツをコンテンツ情報部とコンテンツ本体部にわけ、別々の主体がそれらを管理するため、コンテンツ情報を管理する主体が

コンテンツの内容を確認したうえでコンテンツ情報を受け入れるといった使用方法を導入することが可能となる。第3の効果としては、コンテンツ情報を管理する主体とコンテンツ本体を管理する主体を分離することにより、この2者間で共同でコンテンツを改変しない限りコンテンツの改変は容易に発見することができ、改変を困難にすることが可能となる。

【図面の簡単な説明】

【図1】本発明の構成図である。

【図2】本発明の処理フローである。

【図3】本発明の情報の流れである。

【図4】本発明の一実施例である。

【符号の説明】

11：端末

111：高信頼性通信手段

112：改変確認手段

113：コンテンツ格納手段

114：警告表示手段

12：コンテンツ情報格納部

13：コンテンツ本体格納部

14、15：通信路

10：情報配送元

100：本体配送元

41：端末

411、461：高信頼性通信手段

412：改変確認手段

413：コンテンツ格納手段

414：警告表示手段

42：コンテンツ情報格納部

43：コンテンツ本体格納部

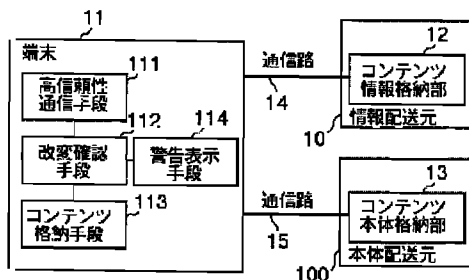
44、45、47：通信路

46：通信センタ

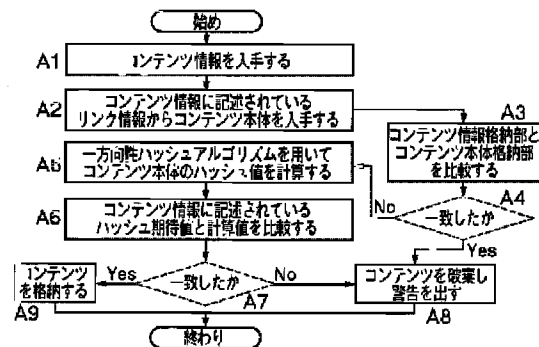
40：情報配送元

400：本体配送元

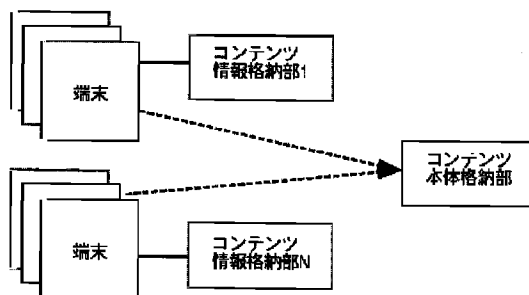
【図1】



【図2】



【図3】



【図4】

